AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

THE PREMISES LOCATED AT: 302 Watson Road, Sullivan, Missouri 63080, located in the Eastern District of Missouri.

Case No. 4:20 MJ 108 DDN

APPLICATION FOR A SEARCH WARRANT

I, Thomas Putting, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized):*

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252, and 2252A	Sexual exploitation of minors

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Applicant's signature

Thomas Putting, Special Agent

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41.

Date: 05/18/2020

/s/ David D. Noce

Judge's signature

City and state: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge

Printed name and title

AUSA: Robert F. Livergood

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT: 302 Watson Road, Sullivan, Missouri 63080, located in the Eastern District of Missouri.	)))))	No. 4: 4:20 MJ 108 DDN FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Thomas Putting, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 302 Watson Road, Sullivan, Missouri 63080 which is located in the Eastern District of Missouri (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations ("HSI"), since March 2019, and am currently assigned to the HSI office in Saint Louis, Missouri. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to search the "SUBJECT PREMISES" which is located at the corner of Watson Road and Hobart Street in Sullivan, Missouri. It is a small two-story residential house made of multicolor stones. The front of the house, which faces north, has two windows on the first floor with one single window in the middle above the front door awning. The front door awning is made of brown wood and has "302" on it in white numbers. The front of the house also has a concrete porch with a metal railing on both sides of the stairs and around the porch. On the west side of the house is a stone chimney. The roof of the "SUBJECT PREMISES" appears to be a brown metal roof that raises into a point in the center of the house. Also, on the south side of the "SUBJECT PREMISES" is a single-story brown garage. A photograph of the home is attached to this Affidavit and labeled as "Attachment A".

4. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted and based on my conversations with other law enforcement officers involved in this investigation.

5. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252, and 2252A are presently located at the "SUBJECT PREMISES", and within computer(s) and related peripherals, computer hardware and media, and wireless telephones found at that location. As a result of the investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Federal law, including 18 U.S.C. §§ 2252, and 2252A, more fully enumerated in the annexed Attachment B, are present at the "SUBJECT PREMISES".

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of 18 U.S.C. §§ 2252, and 2252A, relating to material involving the sexual exploitation of minors.

7. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction

using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

9. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

10. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction

is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geo-located," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

t. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions,

including engaging in online chat, sharing photos or videos, reading a book, or playing a game.

u. "Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

BACKGROUND ON KIK AND KIK REPORTS

11. Kik Messenger (hereinafter, "Kik") is a free instant messaging mobile application designed and previously managed by Kik Interactive Incorporated, a company based in Waterloo, Canada.[1] Kik uses the Internet to allow users to send and receive instant messages, photos and videos, and to engage in video chat. During the account registration process, users are prompted to create a username, which cannot later be changed, and a display name, which other users initially see when communicating. During the registration process, users are also asked to provide an email address, date of birth, user location and a profile picture. Email addresses can be "confirmed," which means the user verified the email address is valid by clicking a link sent from Kik to the provided email address, or "unconfirmed," which means the email address is invalid, or the user did not click on the link from Kik. One key feature of Kik is

[1] Kik was recently purchased by MediaLab, a U.S.-based technology company headquartered in California. At all times relevant to this investigation, Kik was owned by Kik Interactive in Canada.

that users are not required to provide accurate information during the account registration process.

12. Once an account is created, a user is able to locate other users via a search feature. The search feature generally requires a user to know an intended recipient's username to locate them. Once connected, Kik users can share messages, images and videos, or engage in video chat. Kik also allows users to create chatrooms, through which groups of up to 50 users can exchange messages and digital files. These chatrooms, commonly referred to as "Kik Groups," are administered by the user who created the chatroom, and this user has the authority to add, remove and ban other users from the group. These groups are normally created with a group code that contains a "hashtag" (e.g., "#KikTeens"), allowing the group or chatroom to be located more easily. Once a group is created, Kik users can engage in a "group chat" and exchange messages and content.

13. According to Kik's Terms of Service, which each user must acknowledge when creating an account, it is a violation of the agreement to use Kik to upload, post, comment on, or store content that is obscene, offensive, contains pornography, or is harmful to minors in any way. These Terms of Service specifically state that "…[Kik] may review, screen and delete your User Content at any time if we think it may violate these Terms. You are responsible for the User Content that you send through the Services, including for back up of such content."

14. To combat the proliferation of child pornography on its platform, the Kik Trust and Safety Team uses a third-party company to review profile pictures that are uploaded by users and groups. Kik also uses the PhotoDNA software to compare user-uploaded images against a database of known child pornography images that are in circulation. Any images that are flagged and reported by the third-party company or the PhotoDNA software are subsequently viewed by a member of the Kik Trust and Safety Team.

15. Kik also allows users to report other users who have abused or harassed them within the app. These are referred to as "Abuse Reports." When a Kik user submits an Abuse Report, they can include their full conversation history, including text and any images or videos transmitted in the conversation. When the Kik Trust and Safety Team receives an Abuse Report or referral from a third-party moderator, a Kik employee reviews the reported material to verify that it contains child pornography or is otherwise considered child exploitative material.

16. Any material determined by Kik to be exploitative through PhotoDNA hash match, third-party monitoring, or Abuse Reports is subsequently reported to the Royal Canadian Mounted Police (RCMP). Kik provides the RCMP with the reported material, as well as basic subscriber information for the suspect account. This subscriber data includes, but is not limited to, the information entered by the user during the account registration process, any updates to this information after the registration process, device type (e.g., iPhone, Samsung Galaxy S5, etc.), and log-in data associated with the last thirty days of account activity. Upon reporting this information to the RCMP, Kik deletes the suspect account for violating its Terms of Service.

17. Based on my training and experience in child exploitation investigations, I am aware that Kik is a prominent meeting place for individuals seeking to share child pornography and engage in child exploitative dialogue. I have participated in the investigation of offenders who used Kik to transport, distribute, and receive child pornography, as well as other offenders who used the platform to coerce and entice minors to engage in illegal sexual activity. Based on information obtained from interviews with some of these offenders, I am aware that Kik is a preferred platform for child exploitation offenders because the application facilitates anonymous communication, which assists offenders in avoiding detection by law enforcement. This anonymity includes the fact that Kik does not require users to provide accurate subscriber information, which allows offenders to disassociate themselves from the account they access and communicate from.

PROBABLE CAUSE

18. During February of 2020, your affiant reviewed a Kik Report forward from Kik Interactive to Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) (referred to as, C3-CEIU). This Kik report included copies of suspected child pornography which were reviewed by your affiant. These images had previously been located, isolated, searched and viewed by Kik personnel before they were reported to the Royal Canadian Mounted Police (RCMP). Your affiant reviewed only the image previously located, isolated, searched and viewed by Kik personnel and observed that the images is of child pornography as defined by Federal Law.

19. Your affiant reviewed a Kik Report dated September 9, 2019. A review of the report showed that on September 9, 2019, at 16:55:28 UTC a Kik user, who provided the name

of "Tanner Yip," a username of "helix0," and an email address of justice@tahoo.com used Kik to upload an image of child pornography. Additionally, the report listed the device used to register this account as an android "Z971".

20. On or about March 26, 2020, your affiant reviewed the image of child pornography contained within the Report, which was provided to HSI by Kik. The image depicts what appears to be a nude prepubescent female laying down on a grey couch with her legs spread open and her vagina fully exposed. The female is wearing a striped pink and white long sleeve shirt, pink socks, and what appears to be a black undershirt or bra. The female is not wearing any pants or underwear. The female is pulling up her shirt with her right hand and her left hand is touching her vagina. There appears to be a shiny substance all around her vagina and on her left thigh. The female appears to be around eight (8) to ten (10) years of age. Your affiant has learned that Kik was alerted to the described child pornography through use of Kik's PhotoDNA technology.

21. The information provided by Kik included IP addresses associated with access to the pertinent Kik user accounts. Kik provided the IP addresses related to the Kik user's account "helix0". IP address, 72.172.216.245, was the only IP address used for Kik user "helix0" and labeled as WIFI. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that the WIFI IP address 72.172.216.245 is registered to Fidelity Communications Company

22. On March 12, 2020, an HSI administrative summons (Summons number ICE-HSI-SU-2020-00271) was issued to Fidelity Communications Company for the assigned subscriber to IP address 72.172.216.245 used on September 9, 2019 at 16:03:10 UTC.

23. On March 24, 2020, your affiant received information from Fidelity Communications Company regarding summons ICE-HSI-SU-2020-00271. According to the information received relating to IP address 72.172.216.245 gave the following information:

Name:	Andrew ROSE
Address:	302 Watson Rd, Sullivan, MO 63080
Phone Number:	314-629-1088
Account Number:	500115
User ID:	N/A

Email Address:	No Email Given
Customer Status:	Active
Creation Date:	6/15/2018
IP Address:	72.172.216.245
Modem MAC:	688f2e644940
Lease Start:	07/24/2019, 14:01:51
Lease End:	N/A

24. On March 25, 2020, a CLEAR database search revealed that 302 Watson Rd, Sullivan, MO 63080, is listed as the most recent place of residence for Andrew ROSE according to public record.

25. A check with the Department of Motor Vehicles on or about March 25, 2020 revealed that an individual named ROSE with a date of birth of xx/xx/1993 resides at the 302 Watson Rd, Sullivan, MO 63080.

26. A search through government databases showed that ROSE owns a 2009 Chevrolet Impala with Missouri license plate TD1G6F registered to his name. Surveillance of 302 Watson Rd, Sullivan, MO 63080, on or about March 30, 2020 revealed that a 2009 Chevrolet Impala with Missouri license plate TD1G6F at the premises.

27. On or about March 30, 2020, I used my government issued iPhone in an effort to gain additional information regarding any potential wireless networks at 302 Watson Rd, Sullivan, MO 63080. Positioned approximately ten (10) yards from 302 Watson Rd, Sullivan, MO 63080, I noted that there were multiple wireless networks in the area, but all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks, as well as my training and experience and information relayed to me by agents, I believe that the wireless router at 302 Watson Rd, Sullivan, MO 63080, is likely generating a secured wireless network. As explained above, I know, from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

CRIMINAL HISTORY ACTIVITY OF Steven Reich

28. A check on government information systems regarding ROSE revealed that ROSE is a registered sexual offender. A search on ROSE's criminal history revealed that in 2011, ROSE was arrested by the Franklin County Sheriff's Office for possession of child pornography and was prosecuted by the state of Missouri. On or about September 21, 2016, ROSE plead guilty to Possessing Child Pornography-2nd Subsequent Offense or Possess >20 Pictures/One Film/Videotape and sentenced to five (5) years' probation (MO docket number 11AB-CR02379).

CHARACTERISTICS OF INDIVIDUALS WHO RECEIVE AND COLLECT IMAGES OF CHILD PORNOGRAPHY

29. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography collectors typically retain pictures, films, photographs, negatives,

magazines, correspondence, books, tape recordings, mailing lists, child erotica,[2] and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer to have continuous access to their collection of child pornography. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

30. Based upon the conduct of individuals involved in the collection of child pornography set forth above, namely, that they tend to maintain their collections at a secure, private location for long periods of time, there is probable cause to believe that evidence of the offenses of receiving and possessing child pornography is currently located at the premises described previously herein, known as, and the computers and computer media located therein.

SEIZURE OF EQUIPMENT AND DATA

31. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer

---

[2] "Child erotica," as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

32. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense

and is thus subject to immediate seizure as such-- or whether is serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readable, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

33. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

34. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled

environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

35. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED

36. The examination procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC ACCESS

37. This warrant permits law enforcement to compel ROSE to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by

pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES (1) that are known to be used or owned by ROSE, (2) that are subject to seizure pursuant to this warrant, and (3) may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to:

(1) press or swipe the fingers (including thumbs) of ROSE to the fingerprint scanner of the DEVICES found at the premises;

(2) hold the DEVICES found at the premises in front of the face of ROSE and activate the facial recognition feature; and/or

(3) hold the DEVICES found at the premises in front of the face of ROSE and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant.

The proposed warrant does not authorize nor prohibit law enforcement from requesting that ROSE state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize nor prohibit law enforcement from asking ROSE to identify the specific biometric characteristics (including

the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

38. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly access with the intent to view, possess and/or receive child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the subject premises described in Attachment A and known as 302 Watson Road, Sullivan, MO 63080 its storage areas as described on the lease, and any computers, computer media, or wireless telephones therein, and more fully described herein. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and media, and wireless telephones therein.

I state under the penalty of perjury that the foregoing is true and correct.

THOMAS PUTTING
Special Agent
Homeland Security Investigations

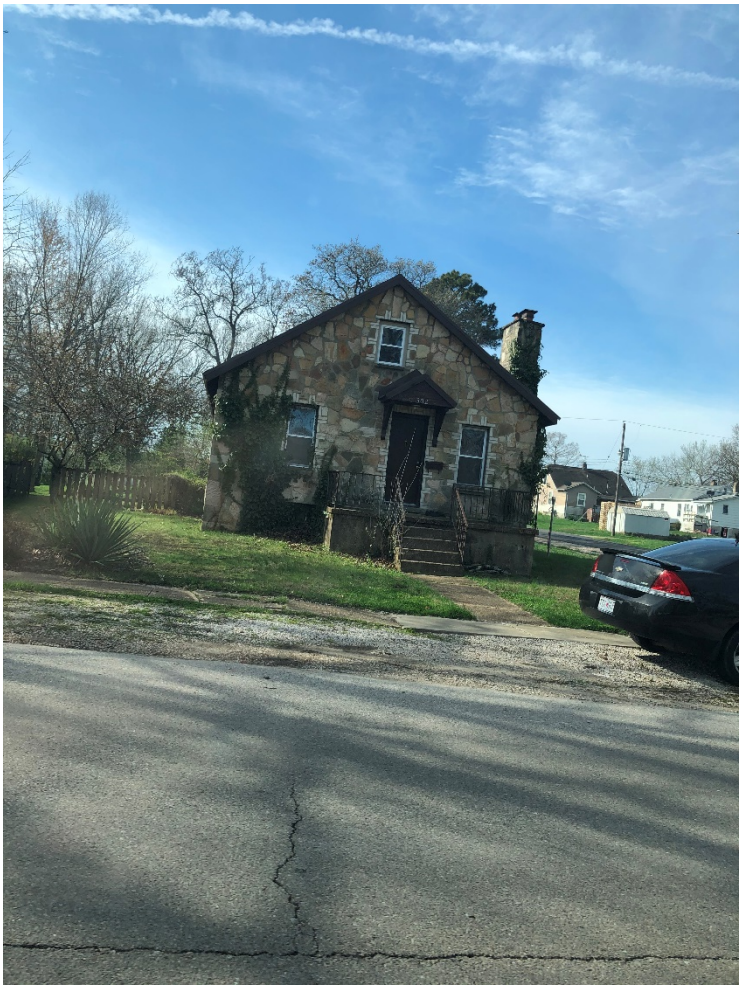
Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this **18th** day of May, 2020.

/s/ David D. Noce
DAVID D. NOCE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

302 Watson Road, Sullivan, MO 63080 is located at the corner of Watson Road and Hobart Street in Sullivan, Missouri. It is a small two-story residential house made out of multicolor stones. The front of the house, which faces north, has two windows on the first floor with one single window in the middle above the front door awning. The front door awning is made of brown wood and has "302" on it in white numbers. The front of the house also has a concrete porch with a metal railing on both sides of the stairs and around the porch. On the west side of the house is a stone chimney. The roof of the 302 Watson Road, Sullivan, MO 63080 appears to be a brown metal roof that raises into a point in the center of the house. Also, on the south side of the 302 Watson Road, Sullivan, MO 63080 is a single-story brown garage.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities and contraband concerning the violations of Title 18, United States Code, Sections 2252 and 2252A, as follows:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

   a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);

   b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

   c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.

6. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

7. During the execution of the search of the Premises described in Attachment A, law enforcement personnel are also specifically authorized to obtain from ANDREW ROSE, if he is located on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the Device(s) found at the SUBJECT PREMISES and known to be owned by or used by ANDREW ROSE;

b. where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.